ABSTRACT

A method of generating a key by a first correspondent. The key is computable by a second correspondent. The method comprises the steps of:

a) making available to the second correspondent a first short term public key;

b) obtaining a second short term public key from the second correspondent;

c) computing a first exponent derived from the first short term private key, the first short term public key, and the first long term private key;

d) computing a second exponent derived from the first short term private key, the first long term public key, the second short term public key and the first long term private key;

computing a simultaneous exponentiation of the first exponent with the second short term public key and the second exponent with the second long term public key.